Winter 12-2-2007

Internet Banking Adoption: The Security Information Perspective

Nena Lim

Proceedings of The Seventh International Conference on Electronic Business, Taipei, Taiwan, December 2-6, 2007, pp. 337-338.

INTERNET BANKING ADOPTION: THE SECURITY INFORMATION PERSPECTIVE

Nena Lim, University of Melbourne, Australia, limn@unimelb.edu.au

ABSTRACT

The objective of this paper is to examine the issue of Internet banking adoption from the perspective of the security information provided by banks on their Web-sites. Security policies provided on the Internet by eight Australian banks were examined and analyzed. Results show that apart from preventive measures, banks hardly disclose any information regarding other aspects of security such as detection. Apart from stating the security measures adopted by banks, most Web-sites have an extensive discussion of banks' expectation of users' roles in security maintenance. It is also interesting to note that while all eight banks expect users to use anti-virus software and firewalls, only two banks indicate they use virus scanning tools.

Keywords: Internet banking, online banking, Internet security.

INTRODUCTION

Internet adoption rate in Australia in 2005 was more than seventy percent but only about thirty percent of the population uses Internet banking. Because of the relatively low adoption rate of Internet banking, studies have been done in Australia and other regions, such as Singapore, Hong Kong, New Zealand, and Scandinavia countries, to examine the antecedents of Internet banking adoption. For example, in a recent study in Australia, 32 Internet users interviewed individually and in focus groups [1]. Their results suggest that factors such as convenience, accessibility, security, privacy, and cost influence participants' Internet banking decision. Moreover, participants would have faith in banks if banks had strong security measures.

RESEARCH QUESTION AND METHODOLOGY

The objective of this paper is to examine the issue of Internet banking adoption from the perspective of the security information provided by banks on their Web-sites. It examines the following research question: What kind of security information is provided by Australian banks on their Web-sites? Security policies provided on the Internet by eight Australian banks were examined and analyzed. They include the four major banks, namely, Commonwealth Bank of Australia (CBA), Australia and New Zealand Banking Group (ANZ), National Australia Bank (NAB), and Westpac Bank, and four other banks as follows: St. George Bank, Suncorp-Metway (Suncorp), Citibank, and HSBC. Results of this study will help banks understand where they stand in comparison to their counterparts in terms of security information provision and might shed light on why Internet users prefer certain banks rather than the others.

RESULTS

Security information provided on banks' Web-sites were analyzed based on three aspects: prevention, detection, and response. Results show that the majority of the information provided by banks is about prevention. All banks implement preventive security measures regarding information storage and transmission. Nevertheless, in terms of detection, results show that only one bank (CBA) indicates it adopts intrusion detection systems. Suncorp is the only bank which indicates it has a backup system in place as an incident response measure.

Information Storage & Transmission

Regarding information storage, more than half of the banks have a clear policy regarding destroy of information, premises security, information access restriction, and computer access control. All but one bank indicate they adopt firewalls. On the other hand, only two banks indicate they de-identify customers' information where appropriate. Moreover, only two banks mention they adopt virus scanning tools or have measures in place against eavesdropping. Also only two banks provide employee training on privacy and confidentiality.

All banks adopt encryption in information transmission and refer their customers to look for a padlock on the browser. Moreover, all but one bank mention their usage of SSL (secure sockets layer) and digital certificates. Yet only three banks tell their customers which certification authority (CA) issues their digital certificates. Half of the banks specify they use 128 bit encryption standard.

Expectation of Users

Apart from stating the security measures adopted by banks, most Web-sites have an extensive discussion of banks' expectation of users' roles in security maintenance. All eight banks expect users to install the latest anti-virus software and firewalls on their computers. All but one bank expect users to install anti-spyware programs. Six banks expect their customers to apply the latest software update and security patches. To facilitate their customers, six banks provide customers with hyperlinks to Web-sites that sell firewalls, anti-virus software, and anti-spyware software. More than half of the banks remind their customers to log off after Internet banking sessions and not to use shared computers to access their Internet bank accounts. Half of the banks expect customers to check last login time and previous transactions to identify any potential problem. Only three remind customers not

to include sensitive personal information in their e-mails.

Additional Security Measures

Some banks provide additional security measures such as secure token or secure SMS (short message services) messages. Citibank provides an on-screen keyboard which is a measure against keyloggers. CBA allows customers to set up an additional login ID which has only restricted access. This facilitates customers who want to check their bank accounts while they travel. Similarly, NAB provides an additional security measure to customers who want to access their Internet bank account while traveling by allowing them to lock their passwords after completion of Internet banking sessions.

CONCLUSION

In summary, all eight Australian banks provide different degrees of detail of security information to their customers. Apart from preventive measures, banks hardly disclose any information regarding other aspects of security such as detection and incident response. It is interesting to note that while all eight banks expect users to use anti-virus software and firewalls, only two banks indicate they use virus scanning tools. While all banks indicate they adopt different security measures such as encryption and digital certificates, most do not explain the terminologies to their customers. Results suggest that banks place a big onus of security on their customers. It is questionable whether such a high level of expectation is realistic because prior research has shown that the e-literacy level of Australian Internet users is not that high. Some banks began to provide two-factor security measures to their customers but the development in this area in Australia is relatively slower than that in other regions such as Europe. The next step of this study is to examine the perceptions of Internet users on such security information and whether their decision to use Internet banking is affected by the security information provided by banks.

REFERENCE

[1] Lichtenstein, S. & Williamson, K. (2006) "Understanding consumer adoption of Internet banking: An interpretive study in the Australian banking context", *Journal of Electronic Commerce Research*, Vol. 7, No.2, pp. 5-66.